UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/870,610	05/31/2001	Dwip N. Banerjee	AUS9-2001-0361-US1	1787

7590 01/24/2005

Joseph T. Van Leeuwen
P.O. Box 81641
Austin, TX 78708-1641

EXAMINER	
BAYARD, DJENANE M	
ART UNIT	PAPER NUMBER
2141	

DATE MAILED: 01/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/870,610	BANERJEE ET AL.	
	Examiner	Art Unit	
	Djenane M Bayard	2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 May 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1, 4, 6, 8, 12, 14, 17 and 19 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,389,532 to Gupta et al.

a. As per claims 1, 8 and 14, Gupta et al teaches a method for preventing malicious network attacks said method comprising: receiving a packet from a client computer (See col. 7, lines 35-37); determining a number of packets received during a time interval (See col. 7, lines 42-44, The number of packets received from the source during the predetermined time period is determined); and rejecting the packet in response to the number of packets exceeding a packet limit (See col. 7, lines 46-47, The router discards the packet is the rate limit has been exceeded).

b. As per claims 4 and 17, Gupta et al teaches the claimed invention as described above. Furthermore, Gupta et al teaches determining an action from a plurality of actions based on the number of packets received; and executing the action (See col. 7, lines 30-

50).

c. As per claims 6, 12 and 19, Gupta et al teaches the claimed invention as described above. Furthermore, Gupta et al teaches creating configuration settings, the configuration settings including the packet limit (See col.7, lines 40-50).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 2-3, 5, 9-11, 15-16 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,389,532 to Gupta et al in view of U.S. Patent Application No. 2002/0101819 to Goldstone.

a. As per claims 2, 9 and 15, Gupta et al teaches the claimed invention as described above. Furthermore, Gupta et al teaches wherein the client computer is identified. However, Gupta et al failed to teach wherein the client computer is identified by a source IP address.

Goldstone teaches prevention of bandwidth congestion in a denial of service or other internet-based attack. Furthermore, Godlstone teaches wherein the client computer is identified by a source IP address (See page 3, paragraph [0039]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate wherein the client computer is identified by a source IP address as taught by Goldstone in the claimed invention of Gupta et al in order to deny future request to connect that are initiated from an attacking client (See page 3, paragraph [0039]).

b. As per claim 3, 10 and 16, Gupta et al teaches the claimed invention as described above. However, Gupta et al failed to teach wherein the determining further includes: identifying a client data area based on a source IP address, the client data area including the number of packets received; and incrementing the number of packets received.

Goldstone teaches identifying a client data area based on a source IP address, the client data area including the number of packets received; and incrementing the number of packets received (See page 3, paragraph [0038]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate identifying a client data area based on a source IP address, the client data area including the number of packets received; and incrementing the number of packets received as taught by Goldstone in the claimed invention of Gupta et al in order for the router to prevent the attacking client from perpetrating further attacks by blocking traffic originating from the attacking client from entering the Internet (See page 3, paragraph [0027]).

c. As per claims 5, 11 and 18, Gupta et al teaches the claimed invention as described above. However, Gupta et al failed to teach receiving a socket request from the client computer; determining a number of sockets opened for the client computer; comparing the number of sockets opened to a socket limit; and determining whether to allow a socket request based on the comparison.

Goldstone teaches prevention of bandwidth congestion in a denial of service or other internet-based attack. Furthermore, Godlstone teaches receiving a socket request from the client computer; determining a number of sockets opened for the client computer; comparing the number of sockets opened to a socket limit; and determining whether to allow a socket request based on the comparison (See page 3, paragraph [0038]).

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate receiving a socket request from the client computer; determining a number of sockets opened for the client computer; comparing the number of sockets opened to a socket limit; and determining whether to allow a socket request based on the comparison as taught by Goldstone in the claimed invention of Gupta et al in order for the router to prevent the attacking client from perpetrating further attacks by blocking traffic originating from the attacking client from entering the Internet (See page 3, paragraph [0027]).

5. Claims 7, 13 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable

over U.S. Patent No. 6,389,532 to Gupta et al in view of U.S. Patent No. 5,892,903 to Klaus.

a. As per claims 7, 13 and 20, Gupta et al teaches the claimed invention as described above. However, Gupta et al failed to teach providing a test script, the test script including one or more attack simulations; processing the attack simulations included in the test script; determining whether to change the configuration settings based on the processing; and changing the configuration settings based on the determination.

Klaus teaches a method and apparatus for detecting and identifying security vulnerabilities in an open network computer communication system. Furthermore, Klaus teaches providing a test script, the test script including one or more attack simulations; processing the attack simulations included in the test script; determining whether to change the configuration settings based on the processing; and changing the configuration settings based on the determination (See col. 9, lines 1-41)

It would have been obvious to one with ordinary skill in the art at the time the invention was made to incorporate providing a test script, the test script including one or more attack simulations; processing the attack simulations included in the test script; determining whether to change the configuration settings based on the processing; and changing the configuration settings based on the determination as taught by Klaus in the claimed invention of Gupta et al in order to detect which computers on a network are susceptible to attacks using predicted TCP sequence numbers (See col. 6, lines 15-20).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,279,113 to Vaidya teaches a dynamic signature inspection-based network intrusion detection.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Djenane M Bayard whose telephone number is (571) 272-3878. The examiner can normally be reached on Monday- Friday 5:30 AM- 3:00 PM..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on (571) 272-3880. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Djenane Bayard

Patent Examiner

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER